09/763103
PCT/GB99/02672

IMPROVEMENTS IN AND RELATING TO DATA COMMUNICATION

Field of the Invention

The present invention relates to data communication devices and methods, and to programs for executing such methods and carriers therefor.

Background to the Invention

With the growth of computer networks, including the internet, local area networks, wide area networks and intranets, additional problems have been created in relation to computer security. In particular, the possibilities for unauthorised remote access into a computer (sometimes referred to as "hacking") have been increased.

Hackers seeking unauthorised access have developed various forms of software to assist in these attacks, including those that make multiple attempts to gain access through password controlled systems. Typically such software will try various permutations of possible passwords until the correct one is found. This can either be a "dictionary" attack, restricted to known words, or a "brute force" attack which tries all permutations. For this reason, amongst others, many systems require passwords of a minimum length, but as these have to be memorised by a user only a certain minimum length is practicable. Thus, many password lengths fall in the range of 4-8 characters and are often everyday words for case of recollection. This makes a software-assisted attack on the system a real risk to any password protected function or data.

It is an aim of preferred embodiments of the present invention to obviate or overcome at least one disadvantage encountered in relation to the prior art, whether referred to herein or otherwise.

Summary of the Invention

According to the present invention in a first aspect, there is provided a method for password enhancing, which method comprises the steps of entering a user password and irreversibly encrypting the user password.

Preferred embodiments of the present invention provide for more secure password handling, by enhancing the password.

Suitably, the encryption comprises a hash operation.

Suitably, the method comprises the additional step of using an encrypted first stored key (NEPKEY) to encrypt the irreversibly encrypted user password (HASH). Suitably, the first stored key is encrypted by a public key encryption algorithm.

Suitably, the method comprises the additional step of decrypting an encrypted second stored key (UPEK) using the decrypted first stored key (NEPKEY). Suitably, the second stored key is encrypted by a reversible algorithm.

Suitably, the result (HASH) of the irreversibly encrypted user password is encrypted using the second stored key (UPEK) as an encryption key.

According to the present invention in a second aspect, there is provided a data access method comprising the steps of producing an enhanced password according to the first aspect of the present invention, comparing the enhanced password with a password associated with the data, and permitting access to the data only if the enhanced password and the data password correspond.

The data to be accessed may be any type, including a file, an application, a data record etc.

According to the present invention in a third aspect there is provided a computer program for carrying out the method of the second aspect of the present invention.

According to the present invention in a fourth aspect, there is provided a carrier comprising a program according to the third aspect of the invention.

According to the present invention in a fifth aspect, there is provided a data communication system comprising an input device for generating a plurality of input signals available from a set of input signals and a character generator configured to receive an input signal and generate an output signal comprising a plurality of signals from the set of input signals in which the output signal is different from the signal input to the character generator.

Suitably, the output signal is of a different length to the signal input to the character generator. More suitably, the output signal is longer than the signal input to the character generator.

Suitably, the system further comprises means for comparing the output signal with a stored password. More suitably, the comparison means further comprises means for outputting a signal dependent upon the correspondence of the output signal with the stored password.

Suitably, the input device comprises a keyboard.

Suitably, the set of available input signals comprises all or part of the character set of the keyboard.

Suitably, the system comprises a first input and a second input in which the character generator receives signals from the first input and does not receive signals from the second input.

Suitably, the first input is a local input device such as a keyboard or microphone and the second input is a remote based input device typically providing signals via a modem connection.

Suitably, the input signal comprises or corresponds to one of the set of input signals.

Suitably, the set of input signals comprises alphanumeric characters.

According to the present invention in a sixth aspect, there is provided a digital computer comprising a data communication system according to the fifth aspect of the invention.

According to the present invention in a seventh aspect, there is provided a data communication method comprising receiving an input signal available from a set of input signals, generating an output signal comprising a plurality of signals from the set of available input signals, in which the output signal is different from the input signal.

Suitably, the method further comprises the step of repeating the operation for a plurality of input signals.

Suitably, the output signals vary in length one from the other.

Suitably, the method according to the eighth aspect of the invention is modified according to the sixth aspect of the invention.

Brief Description of the Drawings

The present invention will now be described, by way of example only, with reference to the drawings that follow; in which:

Figure 1 is a schematic functional illustration of an embodiment of the present invention.

Figure 2 is a functional flow diagram illustrating operation of a preferred embodiment of the present invention.

Figure 3 is a diagram showing how data is stored according to the embodiment of the present invention described in relation to Figure 2.

Figure 4 is a functional flow diagram of the operation of the character generating device of the present invention in another embodiment.

Description of the Preferred Embodiments

Referring to Figure 1 of the drawings that follow, there is shown an electronic digital computer 2, typically a personal computer ("PC") comprising a keyboard 4 connected via a data line 6 to a processor 8. Those skilled in the art will appreciate that various elements intervene between the keyboard and processor.

On the data line 6 between keyboard 4 and processor 8 is a character generating device 10. The initials "CGD" are used for character generating device in this specification.

Other input ports 12, 14 as also shown which may for instance, be from a modem.

The character generating device 10 is configured to controllably modify the output of keystrokes from keyboard 4 to produce additional output for password verification, until that password verification is achieved and then revert to normal keyboard output operation.

The operation of the device will now be described in more detail with reference to Figures 2 onwards of the drawings that follow.

Upon activation of the application a password is requested to be input and the number of characters of an

enhanced password is set. The input is "filtered" to recognise non-character codes such as CTRL and <SHIFT> so that these are not required in the user's password.

Referring now to Figure 2 of the drawings that follow, the keyboard 4, CGD 10 and a PC hard drive 16 are outlined. A user password (PW) is entered from keyboard 4. For purposes of explanation let the user password input be "BOB". The user sets the enhanced password length to, say, 10 characters. Upon an <ENTER> key strike (or typically for a WINDOWS (Registered Trade Mark) application, clicking the "OK" button) the user password BOB is enhanced.

Each CGD 10 contains a common key referred to as a NEPKEY. The CGD 10 uses a secret public key encryption algorithm with its own unique public key (the public key differs between CGD devices) to encrypt the NEPKEY, the result of which, referred to as Spk(NEPKEY) is stored on the PC hard drive. Thus the NEPKEY itself is not known outside of the CGD 10.

The CGD 10 creates a User Password Enchancer Encryption Key, referred to as UPEK, in a function called "GUPEK". A UPEK is generated in the CGD 10 as a random number. It need not be a random number, the main requirement being it is not known outside of the CGD 10. Each CGD 10 has the same NEPKEY (or set of NEPKEYs as several may be used), but a unique UPEK (or set thereof).

GUPEK is passed the Spk(NEPKEY) to be used to encrypt a new UPEK, how many new UPEK's are to within the set, and the location of the temporary resident program that can create UPEKs. It then passed the CGD 10 the encrypted

NEPKEY (ie T_{NEPKEY}(UPEK), where T is a symmetric encryption algorithm). As each new UPEK is created, according to the number to be generated, the CGD 10 encrypts it with the NEPKEY (ie T_{NEPKEY}(UPEK)). When it has finished, the temporary resident program is unloaded from the CGD 10. The CGD 10 then adds the encrypted UPEKs to one block of data, with a header 102 containing how many UPEKs 104a, 104b are within the set, as shown in Figure 3 of the drawings that follow. The NEPKEY encrypted UPEK is saved on the hard drive. Thus the UPEK is not known outside of the CGD 10. The generation of the Spk(NEPKEY) and T_{NEPKEY} (UPEK) are carried out in the set-up stage. There may be several UPEKs in a CGD 10.

At 100 the input user password is hashed to generate an output of predictable length, in this case 16 bytes. The primary reason for the HASH operation is to produce an irreversible result.

In the enhanced password generation method, at 106 the encrypted NEPKEY is retrieved from the PC hard drive 16 and decrypted by the CGD 10 to obtain the NEPKEY. Next at 108 the NEPKEY encrypted UPEK is retrieved and decrypted by the CGD 10 using the NEPKEY decrypted at 106 to obtain the UPEK.

The UPEK is encrypted by the HASH output from 100 and an enhanced password output of desired character length output. This enhanced password is stored, usually in the header portion of an application or document.

When access is sought to the application or document, the password enhancing application is activated and upon a

user password being entered it is password enhanced as set out above, the result being compared with the password stored for the application or document. This comparison is carried out by the application itself, not by the CGD 10 that produces the enhanced password. As a modification the password checking can be carried out by the CGD 10 if it is loaded with appropriate software.

The CGD 10 is configured so that it will only accept one user password per second. The gap between acceptable inputs for password enhancing can be varied to provide additional security.

New NEPKEYs can be entered when required, preferably from a secure source so that the NEPKEY cannot be intercepted.

The HASH operation output length can be varied as a matter of design device. Normally it will be 64 to 128 bytes.

This system has several advantages as set out below:

(i) the user password is not stored on the PC so it cannot be retrieved by a hacker;

(ii) the relationship between the keyboard input and the CGD output (ie the enhanced password) is such that there is no practical reversibility;

(iii) by only permitting one password entry every second or so the system substantially prevents brute force attacks on the password. To succeed in a brute

force attack a large number of permutations must be tried. At one entry per second the time required for a dictionary or brute force attack is unfeasible. For instance, at one million entries per second an six character password, with each character being selected from a possible 72 character set has 139,314,069,504 possible combinations that would take nearly 38 hours to try by brute force. If entry were restricted to one entry per second, the brute force attack would take 4417 years; and

(iv) because of the shared NEPKEY, hot seating (i.e. the use of different machines by one user) can be accommodated even though the CGD 10 on each machine has a different public key. The UPEK('s) associated with the particular user can be transferred securely between machines by encoding using the NEPKEY as a key ie T_{NEPKEY} (UPEK). It is noted that neither the NEPKEY(s) nor the UPEK(s) are seen or inspectable in plain (ie unencrypted) text outside of the secure CGD 10.

If desired new NEPKEYs can be downloaded into the CGD 10 using a security protocol.

A further embodiment of the present invention will now be described with reference to Figure 4 of the drawings that follow.

From a mode 200 in which the PC 2 is operating normally, an access is requested either to functions or data, the PC checks 202 to determine whether the function

or data (say a file) is password protected. If not, the "NO" branch is followed and normal operation resumes with access permitted. If the function or data is password protected, the "YES" branch is followed and a suitable password is requested 204 and the character generating device is configured 206 to output additional characters according to a predetermined scheme.

Then, as each keystroke of the password is input 208 the signal is received by the device 10 and a corresponding longer output is generated 210. Thus, by way of example, if the keystroke "F" is entered, the device may output "P7TTWR0". The actual output is substantially immaterial so long as it is in accordance with a predetermined relationship between the input key and output sequence from the device 10.

The system then determines if the password input is finished 212. This may be by detecting the input of a <ENTER> key, the length of input or some other characteristic . If the input is not finished, the system requires a further input keystroke. If the input is finished, the "YES" branch is followed and the input password is compared with a password in memory 214. If the password is correct, the "YES" branch is followed, the character generator is configured 216 so input passes normally access to the function or data is permitted and normal operation resumed. If the password is incorrect, the "NO" branch is followed and access is denied 218.

Instead of access being denied on the first entry of an incorrect password, several attempts can be permitted, but normally not an unlimited number.

In addition to access being defined upon entry of incorrect password, additional alarm functions may be actuated.

The original password may also be input using this method and device. The user need never know or be concerned with the longer version of their password.

Accordingly, using the present invention it is possible for a user to remember a relatively short password, say "FRED" but for the processor to require validation of a much longer password which may or may not include the original password elements. By way of example, keyboard keystrokes of "FRED" at the password request stage may generate: P7aTWR0X3NR?B2aR88CI9CcAB.

So, a password input keystroke of four characters generates a twenty-six character long password for verification.

The device and system is configured so that remote access to the PC 2 is not via the device 10 so that such remote access requires entry of the full (longer) password required by the processor. Accordingly, protection from external hacking is enhanced.

The present invention can be embodied in hardware and/or software. Typically, in a hardware embodiment the device is located in a keyboard.

The "passwords" referred to herein may be of any signal or combination of signals and need not be "words" at all.

While the present embodiment has been described for use on a PC, it will be appreciated that the present invention can equally be put into effect on other platforms, devices or equipment.

The reader's attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.

All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive.

Each feature disclosed in this specification (including any accompanying claims, abstract and drawings), may be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a generic series of equivalent or similar features.

The invention is not restricted to the details of the foregoing embodiment(s). The invention extends to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any

novel combination, of the steps of any method or process so disclosed.